

PATENT COOPERATION TREATY

BEST AVAILABLE COPY

From the:
INTERNATIONAL SEARCHING AUTHORITY

To:

F B Rice & Co
Level 23
44 Market Street
SYDNEY NSW 2000

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **17 JUN 2005**

Applicant's or agent's file reference
122242

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/AU2005/000487

International filing date (day/month/year)
4 April 2005

Priority date (day/month/year)
2 April 2004

International Patent Classification (IPC) or both national classification and IPC
Int. Cl. ⁷ H04L 9/32, 9/30, 12/58, 12/66

Applicant

COLLA, Gregory Alan et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the IPEA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. (02) 6285 3929

Authorized Officer

ROBERT BARTRAM

Telephone No. (02) 6283 2215

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

10/594986
IAP2 Rec'd PCT/PTO 29 SEP 2006

International application No.

PCT/AU2005/000487

Box No. I Basis of the opinion

1. With regard to the language, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).
2. With regard to any nucleotide and/or amino acid sequence disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material
☐ a sequence listing
☐ table(s) related to the sequence listing
 - b. format of material
☐ in written format
☐ in computer readable form
 - c. time of filing/furnishing
☐ contained in the international application as filed.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority for the purposes of search.
3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/AU2005/000487

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1 to 66	YES
	Claims	NO
Inventive step (IS)	Claims	YES
	Claims 1 to 66	NO
Industrial applicability (IA)	Claims 1 to 66	YES
	Claims	NO

2. Citations and explanations:

- D1) Herbert A, "End-to-End security over the internet: Deliverable D1 – Implementation Architecture",
D2) WO 2000/045539
D3) Chihara et al, "PGP-Based security enhanced mail gateway (SEMAIL) with POP Authentication for large scale organizations"
D4) WO 2001/008377
D5) US 5943426
D6) JP 11-196080

Novelty:

All of the claims are considered to be novel because none of the documents listed disclose all of the features defined in any of the claims. In particular providing a key container by a key container directory, the key container to be used to secure a message that will be sent from a sender to a recipient, wherein a request for a key container is received from the requestor, a key container is provided to the requestor that contains a cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

Inventive Step:

The novel feature indicated above is the key container directory. In the Claims the terminology "key container" is interpreted to be the data sent that contains the encryption key. It may also contain other data but merely calling this a key container does not provide any other functional meaning than the data transmitted includes the key. D1 discloses end to end security over the internet and specifically at page 47 part 7.1 discloses a secure mail gateway that provides signing and signature verification driven by the senders name and encryption of confidential messages. D1 does not explicitly disclose the use of a key container directory. Directories for encryption keys are well known in the art of secure data communication systems and an example of this can be found in D6. To implement a simple directory as a means to look up a key to use is considered part of the common general knowledge of the art and as such to implement such an alternative to that disclosed in D1 is considered to be no more than a minor workshop improvement that would be implemented without invention. As a result the independent claims are all considered to be lacking an inventive step. The features added by the dependent claims all appear to be minor variations to the concept defined in the independent claims and as such these claims are all considered to be either disclosed or part of the common general knowledge in the art. For example remote directories, determining the type of key container, determining the domain, parameters to determine key use, and the use of time dependent keys are all well known options in secure communications that would be implemented without invention to D1.

Cont. on supplemental sheet.

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/AU2005/000487

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Based on the disclosure of your priority documents I was not able to locate any reference to the features introduced in claims 31 to 33 and 66, the time dependent conditions on the key, claim 35, 39, 52, 56, and 59, the parameter that indicates the key container use, or claim 42 and 62 security preferences of the gateway. As such these claims appear to introduce features that are not fully supported by the disclosure of the priority documents.

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International Application No.

PCT/AU2005/000487

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of: Box V.2

D2 discloses all of the feature you have defined in all of your claims except for the fact that it is directed towards IP telephony. The CTAs function equivalently to your disclosed gateways and a remote gateway controller is clearly disclosed. D2 is in the field of secure communications and a person skilled in the art of secure communication systems would have considered it relevant, ascertained and understood it. Furthermore the obvious combination of D2 with D1 is considered to disclose all of the features you have defined in all of your claims 1 to 66 rendering your claimed invention as not inventive.